(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 982 688 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
01.03.2000 Bulletin 2000/09

(51) Int Cl.[7]: **G07C 9/00**

(21) Application number: **99810764.3**

(22) Date of filing: **25.08.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **26.08.1998 EP 98810845**

(71) Applicant: **Datamars SA**
6930 Bedano-Lugano (CH)

(72) Inventor: **Stegmaier, Peter A. Dr.**
6946 Ponte Capriasca (CH)

(74) Representative:
AMMANN PATENTANWÄLTE AG BERN
AMMANN INGENIEURS-CONSEILS EN PROPRIETE INTELLECTUELLE SA BERNE
AMMANN PATENT ATTORNEYS LTD BERNE
Schwarztorstrasse 31
Postfach
3001 Bern (CH)

(54) Method for preventing or detecting fraud in an identification system

(57) In an identification system comprising a transponder attached or associated to an object and means for reading the identifying code memorised in this transponder, additional information such as a serial number of the chip used in the transponder is memorised and transmitted with the code during reading of the transponder. In this way, fraudulent copying of transponders is prevented and/or detection of such copies improved.

EP 0 982 688 A1

Description

[0001] This invention relates to a method according to the preamble of claim 1. Identification systems of this type are well known, for instance from US-patent 2 293 399. The objects to be identified by such systems may be of any kind, but they often are animals, for instance as described in US-patent 5 211 129. No specific means are disclosed in the patent specifications mentioned above for preventing or at least detecting fraud by copying transponders wherein the identification code of some valuable object such as an animal is stored.

[0002] The transponders usually make use of integrated circuits (chips) as active elements. Of these chips mainly three versions exist:

- the laser programmed on wafer level. These chips can be looked at as invariant.
- the OTP versions (one time programmable). These chips are programmed sometimes before being put into the object to be identified and their memory content cannot be changed afterwards.
- the read/write (R/W) versions. These chips can, at least partially, be reprogrammed at any time.

[0003] Fraud by copying the code of a specific transponder into an OTP or R/W transponder in order to obtain two identical transponders can occur and needs to be made impossible. One well known approach is to use a secret key and some cryptographic algorithm (symmetric or asymmetric) to generate a cyphrate out of a random number sent to the transponder as challenge. The cryphrate is sent back from the transponders to the reader. Often the code of the transponder is also used as input to the cryptographic algorithm. Knowing algorithm and secret key (or public key in asymmetric systems) the reader can authenticate the transponder at any time. This method, however needs to make use of at least one secret key which needs to reside within the transponder memory and therefore requires sophisticated key handling.

[0004] EP-A-0 689 150 discloses a somewhat less sophisticated system, wherein a radio time signal received at reading time as well by the transponder as by the interrogating station. This time signal is combined with the identification code and retransmitted from the transponder to the interrogating station where the information retransmitted is analysed for reading the code. However, transponders are often passive elements without power source, the power for retransmission of the information being provided by the interrogating signal received by the transponder. It is impossible under these circumstances to continuously run a time clock in the transponder, and it is hardly possible to receive a radio time signal without power source in the transponder. Further, without cryptographic treatment of the time signal and code it would be possible for foreigners to determine the addition of a time signal and the code from the response signal of the transponder and thus to copy the transponder.

[0005] This invention aims in providing security against copying without reaching the level of cryptography and without increased power requirement. This security is obtained by the characterising features of claim 1.

The advantage of this method is that it is not requiring complicated and error prone key handling and requires almost no computing power. The latter in contrast to cryptographic methods. Preferably, the method makes use of a chip serial number that makes the combination of the code and the chip serial number almost unique as long as the respective chip manufacturer never produces two identical serial numbers. By registering code and serial number in a database or a certificate that holds the data of the object to be identified and is kept separate from the object a simple copy operation into readily available OTP transponders becomes impossible.

[0006] However, to make sure that attempting fraud using chips with programmable serial numbers is recognised, a database can be used at identification set-up time when the code/serial number pair is stored into the database. At this moment, the database can be searched for double serial numbers and/or codes.

[0007] To make the serial number even more specific, a chip manufacturer identification (ID) may also be associated to the chip and made part of the serial number using the above method.

[0008] To avoid the need for reading long serial numbers a checksum type information (e.g. CRC) can be generated from the serial number and used for the above mechanism instead of the serial number. This however may reduce security. If the checksum type number is calculated over code, serial number etc. or over portions of the memory or over the whole memory, it permits consistency checking of the respective information as long as the algorithm for the checksum type number is kept secret.

[0009] This identification of the manufacturer or the user of the chip may be a trademark such as the registered trademark RID of applicant.

[0010] With every code read a geographic information etc. can be stored into the database along with time and date of the read operation to facilitate plausibility checks. Other and additional information may be stored in the memory of the transponder. A possible method is described below, whereby additional information mentioned therein may be omitted or replaced by other specific information.

Detailed description of th Method based on the example of ISO 11 784/85 transponders:

[0011] At die production time a unique die serial

number and a die manufacturer identification (ID) are attributed to every die.

[0012] At code programming time the code, the die serial number, and the die manufacturer-ID are combined into a consistency check number using a specific method, e.g. a CRC scheme. The resulting number is programmed into the memory of the transponder, e.g. in the trailer bits and needs to be stored in the respective database or marked down in the animals passport, etc. for subsequent consistency check.

[0013] At code read time the code, the die serial number, the die manufacturer-ID, and the consistency check number are read and the same method is applied to check consistency of all respective numbers. Then comparing the consistency check number (i.e. the number stored in the trailer bits) with the respective number in the database, in the animals passport, etc. the tag (transponder) can be authenticated.

[0014] This method can prevent from copying transponders as long as no OTP dies are available that allow the programming of die serial number and die manufacturer-ID at code programming time.

[0015] By storing of the respective information into a database with access limited to authorised personnel the copying of serial numbers can often be detected.

[0016] From the above specification and from the following claims it results that substantially two basic solutions are available. The first solution is based upon an information stored outside the transponder and the interrogating station, this information being not accessible during transmission of the response from the transponder, and said information being invariable and being used as a check basis (claim 2).

[0017] The second solution is based onto a consistency test of two or more data stored within the transponder, these data being connected by an algorithm outside the transponder (claim 3). Therefore, no algorithm or key has to be stored in the transponder.

[0018] Of course, any combination of the first and second solution is feasible. A number of additional or alternative measures are possible, for instance as set out hereinafter.

[0019] Preferably the previous registration at identification set-up time may be compared to the information retrieved from the transponder at code-read time to discover fraud by modification of said information or fraud by copying the transponder using blank chips and copying the code leading to different serial numbers. This allows explicit authentification at any time.

[0020] Further, a checksum type information may additionally be stored in a database not accessible by fraudulent personnel.

[0021] The method for generation of a checksum type information may be a hashing function calculated from any portion of the transponder memory. The method for the generation of the checksum type information may also be a cryptographic function calculated from any portion of the transponder memory and making use of symmetric or asymmetric keys and where only the results of the respective calculations are stored in the memory of the transponder but not said keys. Hereby, it is of importance that no key has to be stored in the transponder.

[0022] Another possibility is to store any additional information in the memory of the transponder in such a way that the boundaries of the individual numbers of the stored additional information are not distinguishable to the not knowing. In this way the boundary between the checksum type information and the remaining information shall be obliterated in order to protect the checksum type information from fraudulent analysis.

Claims

1. A method for preventing or detecting fraud in an identification system wherein a transponder having a memory comprising an identifying code is associated with an object to be identified, this transponder being activated by an interrogating signal for transmission of said code, the so received code being used through registration of the code along with object information for identification of said object, characterised in that at least one additional information useful for the determination of the uniqueness of the transponder is memorized in said memory, authentication of identification of said object being based onto the combination of said code and said additional information.

2. The method of claim 1, wherein said additional information is registered together with said code, authentication comprising comparison of said memorized code and additional information with said registered code and additional information.

3. The method of claim 1, wherein a consistency check is based on additional information memorized in the transponder.

4. The method of claim 2 or 3, wherein said additional information is a representation of the manufacturers name or trademark.

5. The method of claim 2 or 3, wherein said additional information is memorised during manufacturing of the transponder chip as a unique chip serial number which cannot be altered by the programmer of the transponder code.

6. The method of claim 5, comparing the previous registration at identification set-up time, where the code and serial number are registered, for double serial numbers to discover fraud by using chips which allow or enable programmable serial numbers.

7. The method of claim 1 or 5, comparing the previous registration at identification set-up time to the information retrieved from the transponder at code-read time to discover fraud by modification of said information or fraud by copying the transponder using blank chips and copying the code leading to different serial numbers.

8. A method according to any one of claims 1 - 3 and 5 - 7, comprising integrating a die manufacturer ID into the serial number to avoid double serial numbers from different manufacturers.

9. A method according to claim 5, comprising using a checksum type information made out of the serial number, e.g. to gain time in reading the shorter checksum instead of the serial number.

10. A method according to claim 9, comprising using a checksum type information made out of the serial number and a manufacturer identification (ID), e.g. to gain time in reading the shorter checksum instead of the serial number and manufacturer ID.

11. A method according to claim 10, wherein the checksum type number is made out of the serial number, the manufacturer identification (ID), and the code in order to permit a consistency check over code, serial number, ID, and checksum type of information.

12. Method according to claim 3, where a checksum type number is calculated over any portion or the whole memory of the transponder in order to enable a consistency check.

13. A method according to claim 3, 10, 11 and 12, comprising storing the checksum type information also into the transponder so that multiple different information are obtained: code, serial number, manufacturers ID, and checksum, e.g. reading all multiple information as well as the checksum type information at authentication time allowing to check consistency.

14. A method according to claim 2 and 5, comprising storing code and serial number in a database not accessible by fraudulent personnel.

15. A method according to claim 14, comprising additionally storing manufacturer ID in a database not accessible by fraudulent personnel.

16. A method according to claim 9, 10, 11, 12 or 13, comprising additionally storing the checksum type information in a database not accessible by fraudulent personnel.

17. A method according to any one of claims 1 to 14, wherein said code and said additional information are registered in a database or in a certificate not accessible to non-authorised persons or in a computer database with write access only to authorized persons, in order to permit the search for double information or inconsistent information to detect fraudulent action at any time using said database or certificate.

18. A method according to claim 17, making use of time information, geographical information, information on the code-reading person or organisation and so on, gathered during code-read time and making plausibility checks possible in order to detect copies of transponders.

19. A method according to any one of claims 1 to 18, where the method for the generation of the checksum type information is a hashing function calculated from any portion of the transponder memory.

20. A method according to any one of claims 1 to 19, where the method for the generation of the checksum type information is a cryptographic function making use of symmetric or asymmetric keys and where only the results of the respective calculations are stored in the memory of the transponder but not said keys.

21. A method according to any one of claims 1 to 20, where any additional information stored in the memory of the transponder is stored in such a way that the boundaries of the individual numbers of the stored additional information are not distinguishable to the not knowing.

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 81 0764

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	DE 197 03 999 A (BOSCH GMBH ROBERT) 6 August 1998 (1998-08-06)	1	G07C9/00
A	* claim 1; figure 1 *	2-21	
Y	US 5 028 918 A (GILES THOMAS E ET AL) 2 July 1991 (1991-07-02)	1	
A	* claim 1; figure 1 *	2-21	
A	EP 0 689 150 A (ALCATEL AUSTRIA AG) 27 December 1995 (1995-12-27) * claim 1; figure 1 *	1-21	
A	GB 2 164 825 A (SATELLITE VIDEO SYSTEMS LTD) 26 March 1986 (1986-03-26) * claim 1; figure 1 *	1-21	
A	US 5 166 676 A (MILHEISER THOMAS A) 24 November 1992 (1992-11-24) * claim 1; figure 1 *	1-21	
A	EP 0 600 556 A (NEDAP NV) 8 June 1994 (1994-06-08) * claim 1; figure 1 *	1-21	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G07C G06K

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	21 December 1999	Kirsten, K

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 81 0764

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-12-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19703999 A	06-08-1998	AU 6608998 A	25-08-1998
		WO 9834200 A	06-08-1998
		EP 0891606 A	20-01-1999
US 5028918 A	02-07-1991	NONE	
EP 0689150 A	27-12-1995	NONE	
GB 2164825 A	26-03-1986	NONE	
US 5166676 A	24-11-1992	US 4730188 A	08-03-1988
		US 5041826 A	20-08-1991
		AT 69533 T	15-11-1991
		AU 4062285 A	10-09-1985
		CA 1264840 A	23-01-1990
		DE 3584651 A	19-12-1991
		EP 0171433 A	19-02-1986
		JP 60171475 A	04-09-1985
		WO 8503831 A	29-08-1988
EP 0600556 A	08-06-1994	NL 9202069 A	16-06-1994

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82